CLAIMS

1. A method used in the control of a physical system, comprising the steps of

(a) modelling a risk chain, the risk chain being a series of two or more entities that each model a discrete part of how a threat leads to damage to a target system, each entity being described as a population of elements distributed in a parameter or parameters, each entity generating the next entity in the chain; and

(b) controlling the physical system by using results of the modelling.

2. The method of Claim 1 in which the way one entity in the risk chain generates another entity in the risk chain is described by a quantitative generation function.

3. The method of Claim 1 or 2 comprising the further step of modelling countermeasures to one or more entities in the risk chain, each countermeasure being quantitatively described as a function of one or more variables.

4. The method of Claim 3 comprising the further step of deploying a countermeasure to an entity in such a manner so that the effect of the entity is diminished to a defined, quantitative level.

5. The method of any preceding Claim 3 or 4 in which the or each variable describing a countermeasure determines the efficacy of that countermeasure in modifying the population of elements in an entity or influencing how one entity in the risk chain generates another entity in the risk chain.

6. The method of Claims 3, 4 or 5 in which the deployment of countermeasures is quantitatively optimised.

7. The method of any preceding Claim in which the distribution of elements of an entity in a parameter is a measured distribution.

8. The method of Claim 7 in which the measured distribution is a real-time measured distribution.

9. The method of Claim 7 or 8 in which the measured distribution is compared to a predicted distribution, the comparison enabling the accuracy of an algorithm used to make the prediction to be improved.

10. The method of any preceding Claim in which the controlled system is controlled by being dynamically altered on the basis of the modelling.

11. The method of Claim 10 in which the controlled system is dynamically altered based on measurements of the distribution of elements in one or more parameters.

12. The method of any preceding Claim in which each entity in the risk chain is an entity with substantially the properties of an entity selected from the following list of entity types: threat agents; attacks; security breaches; disruptions; damage.

13. The method of Claim 12 when dependent on any of Claims 3 - 6 in which the countermeasure that modifies the threat agent entity or influences the output of that entity is an ameliorative measure.

14. The method of Claim 12 when dependent on any of Claims 3 - 6 in which the countermeasure that modifies the attack entity or influences the output of that entity is a resistive measure.

15. The method of Claim 12 when dependent on any of Claims 3 - 6 in which the countermeasure that modifies the security breach entity or influences the output of that entity is a mitigative measure.

16. The method of Claim 12 when dependent on any of Claims 3 - 6 in which the countermeasure that modifies the disruption entity or influences the output of that entity is an alleviative measure.

17. The method of any preceding Claim in which the target system is a computer.

18. The method of any preceding Claim 1-16 in which the target system is a computer network.

19. The method of any preceding Claim 1-16 in which the target system is a telecommunication system.

20. The method of any preceding Claim 1-16 in which the target system is a mobile communications device or personal digital assistant.

21. The method of any preceding Claim 1-16 in which the target system is a building, group of buildings, physical infrastructure, means of transport or a transport infrastructure, aircraft or vehicle.

22. The method of any preceding Claim 1-16 in which the target system is a physical storage container.

23. The method of any preceding Claim 1 – 16 in which the target system is a business, business process or business system.

24. The method of any preceding Claim in which an entity in the risk chain describes a population of one or more people who seek or otherwise obtain unauthorised access to the target system or who seek to or otherwise influence it in an unauthorised manner.

25. The method of any preceding Claim 1-23 in which an entity in the risk chain describes a population of one or more computer viruses or worms or Trojan Horses or computers.

26. The method of Claim 25 in which a parameter is the age of the virus.

27. The method of any preceding Claim 1-23 in which an entity of the risk chain describes a population of one or more fires, floods, earthquakes or other physical acts which have an impact on the target system.

28. A method of modelling a specific security threat to a system, comprising the step of modelling a risk chain, the risk chain being a series of two or more entities that each model a discrete part of how a threat leads to damage to the system, each entity being described as a population of elements distributed in a parameter or parameters, each entity generating the next entity in the chain.

29. The method of Claim 28 in which the way one entity in the risk chain generates another entity in the risk chain is described by a quantitative generation function.

30. The method of Claim 28 or 29 comprising the further step of modelling countermeasures to one or more entities in the risk chain, each countermeasure being quantitatively described as a function of one or more variables.

31. The method of Claim 30 comprising the further step of deploying a countermeasure to an entity in such a manner so that the effect of the entity is diminished to a defined, quantitative level.

32. The method of any preceding Claim 30 or 31 in which the or each variable describing a countermeasure determines the efficacy of that countermeasure in modifying the population of elements in an entity or influencing how one entity in the risk chain generates another entity in the risk chain.

33. The method of Claims 30, 31 or 32 in which the deployment of countermeasures is quantitatively optimised.

34. The method of any preceding Claims 28 – 33 in which the distribution of elements of an entity in a parameter is a measured distribution.

35. The method of Claim 34 in which the measured distribution is a real-time measured distribution.

36. The method of Claim 34 or 35 in which the measured distribution is compared to a predicted distribution, the comparison enabling the accuracy of an algorithm used to make the prediction to be improved.

37. The method of any preceding Claims 28 - 36 in which the system is controlled by being dynamically altered on the basis of the modelling.

38. The method of Claim 37 in which the controlled system is dynamically altered based on measurements of the distribution of elements in one or more parameters.

39. The method of any preceding Claims 28 - 38 in which each entity in the risk chain is an entity with substantially the properties of an entity selected from the following list of entity types: threat agents; attacks; security breaches; disruptions; damage.

40. The method of Claim 39 when dependent on any of Claims 30 - 33 in which the countermeasure that modifies the threat agent entity or influences the output of that entity is an ameliorative measure.

41. The method of Claim 39 when dependent on any of Claims 30 - 33 in which the countermeasure that modifies the attack entity or influences the output of that entity is a resistive measure.

42. The method of Claim 39 when dependent on any of Claims 30 - 33 in which the countermeasure that modifies the security breach entity or influences the output of that entity is a mitigative measure.

43. The method of Claim 39 when dependent on any of Claims 30 - 33 in which the countermeasure that modifies the disruption entity or influences the output of that entity is an alleviative measure.

44. The method of any preceding Claims 28 - 43 in which the system is a computer.

45. The method of any preceding Claims 28 - 43 in which the system is a computer network.

46. The method of any preceding Claims 28 - 43 in which the system is a telecommunication system.

47. The method of any preceding Claims 28 - 43 in which the system is a mobile communications device or personal digital assistant.

48. The method of any preceding Claims 28 - 43 in which the system is a building, group of buildings, physical infrastructure, means of transport or a transport infrastructure, aircraft or vehicle.

49. The method of any preceding Claims 28 - 43 in which the system is a physical storage container.

50. The method of any preceding Claims 28 - 43 in which the system is a business, business process or business system.

51. The method of any preceding Claims 28 - 50 in which an entity in the risk chain describes a population of one or more people who seek or otherwise obtain unauthorised access to the target system or who seek to or otherwise influence it in an unauthorised manner.

52. The method of any preceding Claims 28 - 50 in which an entity in the risk chain describes a population of one or more computer viruses or worms or Trojan Horses or computers.

53. The method of Claim 52 in which a parameter is the age of the virus.

54. The method of any preceding Claims 28 - 50 in which an entity in the risk chain describes a population of one or more fires, floods, earthquakes or other physical acts which have an impact on the target system.

55. A computer network controlled using the method of any preceding Claim 1 – 27.

56. A computer network designed using the method of any preceding Claim 28 - 54.

57. A physical system controlled using the method of any preceding Claim 1 – 27, in which the physical system is a system selected from the following list: a telecommunication system; a mobile communications device or personal digital assistant; a building, group of buildings, physical infrastructure, means of transport, transport infrastructure, aircraft or vehicle; a physical storage container.

58. A physical system designed using the method of any preceding Claims 28 - 54, in which the physical system is a system selected from the following list: a telecommunication system; a mobile communications device or personal digital assistant; a building, group of buildings, physical infrastructure, means of transport, transport infrastructure, aircraft or vehicle; a physical storage container.

59. A method of insuring against risk or underwriting risk using the method of any preceding Claims 28 - 54.

60. A method of pricing insurance risk using the method of any preceding Claims 28 - 54.

61. The method of preceding Claim 59 or 60 in which the risk is digital risk.

62. A countermeasure when calibrated with a quantitative measure of efficacy using the method as defined in any of Claim 28 - 54, in which the quantitative measure is the efficacy of that countermeasure in modifying the population of elements in an entity or influencing how one entity in the risk chain generates another entity in the risk chain.

63. A method of calibrating a countermeasure with a quantitative measure of efficacy using the method as defined in any of Claims 28 - 54, in which the quantitative measure is the efficacy of that countermeasure in modifying the population of elements in an entity or influencing how one entity in the risk chain generates another entity in the risk chain.

64. A method of representing a threat comprising the steps of

(a) modelling that threat using the method of any of Claims 28 - 54;

(b) sending information representing the modelled threat over a wide area network;

(c) displaying that information on a computer connected to the network.